Datenschutzrechtliche Rahmenbedingungen

Zu den datenschutzrechtlichen Vorgaben für öffentliche Organe des Bundes und der Kantone

Astrid Epiney[*]

Dieser Beitrag wurde erstmals wie folgt veröffentlicht:
***Astrid Epiney*, Datenschutzrechtliche Rahmenbedingungen – Zu den datenschutzrechtlichen Vorgaben für öffentliche Organe des Bundes und der Kantone, in: Schweizerische Vereinigung für Verwaltungsorganisationsrecht (Hrsg.), Verwaltungsorganisationsrecht – Staatshaftungsrecht – öffentliches Dienstrecht. Jahrbuch 2010, Bern 2011, S. 5-34. Es ist möglich, dass die Druckversion – die allein zitierfähig ist – im Verhältnis zu diesem Manuskript geringfügige Modifikationen enthält.**

I. Einleitung und Problemstellung

In Sozial- und Bildungsinstitutionen wird selbstredend eine Reihe von persönlichen Daten bearbeitet, womit die Frage aufgeworfen wird, welche rechtlichen Vorgaben hier zu beachten sind. Dabei ist die Problematik schon insofern sehr vielschichtig, als die Träger solcher Institutionen variieren, die spezifischen Rechtsgrundlagen in sehr unterschiedlicher Form ausgestaltet sind und die Art der Datenbearbeitung sowie der bearbeiteten Daten ebenfalls von Fall zu Fall differieren. Diese Situation bringt es auch mit sich, dass für die verschiedenen, sich in dem grossen Komplex „Datenbearbeitung in Sozial- und Bildungsinstitutionen" möglicherweise stellenden Probleme bzw. Fragen durchaus sehr unterschiedliche Rechtsgrundlagen zur Anwendung kommen können.

Vor diesem Hintergrund kann es im Folgenden nicht darum gehen, in irgendeiner Form erschöpfend die datenschutzrechtlichen Vorgaben im Rahmen der Tätigkeiten von und in Sozial- und Bildungsinstitutionen zu behandeln. Vielmehr geht es darum, die grossen datenschutzrechtlichen Grundsätze aufzuzeigen, die bei der Frage nach den konkret einschlägigen datenschutzrechtlichen Vorgaben zu beachten sind. Diese sollen bzw. können dann die Grundlage für die Beantwortung konkreter datenschutzrechtlicher Fragen bilden.[1]

In diesem Sinn sollen im Folgenden – auf der Grundlage einer Skizzierung von Zielsetzung und Problematik des Datenschutzes und des Datenschutzrechts (II.) – einigen besonders wichtigen Grundbegriffen des Datenschutzrechts (III.), dem anwendbaren Recht (IV.) und den relevanten datenschutzrechtlichen Grundsätzen (V.) nachgegangen werden, dies auch unter

---

[*] Herrn MLaw Thomas Meier sei herzlich für die Hilfe bei der Materialsuche gedankt.

[1] Dabei erfolgt bei den allgemeinen Ausführungen in diesem Beitrag teilweise eine Anlehnung an ASTRID EPINEY/TAMARA CIVITELLA/PATRIZIA ZBINDEN, Datenschutzrecht in der Schweiz. Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Freiburger Schriften zum Europarecht Nr. 10, 2009.

Rückgriff auf konkrete Beispiele und Anwendungsfälle. Der Beitrag schliesst mit einer kurzen Schlussbemerkung (VI.).

II. Datenschutzrecht: Problematik und verfassungsrechtliche Rahmenbedingungen

Datenschutz und datenschutzrechtliche Regelungen sind vor dem Hintergrund zwei komplementärer Interessen bzw. Anliegen zu sehen:

- Erstens stellt der Datenschutz einen Teilgehalt des **Rechts auf Schutz der Privatsphäre und der Persönlichkeit** dar, da dem Einzelnen das Recht zukommt, über die Zulässigkeit der Verarbeitung ihn betreffender Daten zu entscheiden. So erfasst der Schutzbereich des Art. 8 EMRK die Erhebung und Speicherung personenbezogener Daten sowie ihre Verwertung und Übermittlung. Einschränkungen der Garantie des Art. 8 Abs. 1 EMRK müssen den eng auszulegenden Anforderungen des Art. 8 Abs. 2 EMRK entsprechen (gesetzliche Grundlage, Rechtfertigung aus einer der in Art. 8 Abs. 2 EMRK explizit aufgeführten Gründe sowie Verhältnismässigkeit).[2]

  In der Bundesverfassung verankert **Art. 13 BV** neben dem Anspruch auf Achtung des Privatlebens (einschliesslich der Wohnung) sowie des Brief-, Post- und Fernmeldeverkehrs auch allgemein einen **Anspruch jeder Person auf „Schutz vor Missbrauch ihrer persönlichen Daten"**.[3] Der **Schutzbereich des Art. 13 Abs. 2 BV** umfasst – was in der etwas missglückten Formulierung nicht wirklich zum Ausdruck kommt – tatsächlich ein **Grundrecht auf informationelle Selbstbestimmung**, so dass jeder Umgang mit personenbezogenen Daten erfasst ist. Allerdings kann dieses Grundrecht unter Wahrung der Vorgaben des Art. 36 BV (gesetzliche Grundlage, öffentliches Interesse oder Schutz von Grundrechten Dritter, Verhältnismässigkeit sowie Wahrung des Kerngehalts) eingeschränkt werden.
- Auf der anderen Seite stellt Datenschutz aber auch ein eminent **öffentliches Interesse** dar. Denn ein demokratischer Rechtsstaat kann nur funktionieren, wenn Staat und Private nicht die Befugnis haben, beliebige personenbezogene Daten nach Gutdünken zu erheben und zu verwerten, wird doch damit der Bürger nicht (mehr) als

---

[2] Vgl. ausführlich hierzu m.w.N. ASTRID EPINEY/BERNHARD HOFSTÖTTER/ANNEKATHRIN MEIER/SARAH THEUERKAUF, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen. Zur rechtlichen Tragweite der europa- und völkerrechtlichen Vorgaben und ihren Implikationen für die Schweiz, 2007, 36 ff. S. auch GABRIELE BRITZ, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, 1 ff.; CHRISTOPH GRABENWARTER, Europäische Menschenrechtskonvention, 2008, 189 ff.

[3] Damit wird – wie übrigens auch in Art. 8 der Grundrechtecharta – der Schutz personenbezogener Daten vom Schutz der Privatsphäre losgelöst und unabhängig von dem Vorliegen eines Eingriffs in dieselbe als eigenständiges Schutzgut definiert. Insofern kann man hier von einer zweiten Generation datenschutzrechtlicher Regelungen sprechen, die – im Gegensatz zu der etwa in Art. 8 EMRK zum Ausdruck gekommenen ersten Generation – Datenschutz als eigenständiges Ziel unabhängig von einem Eingriff in die Privatsphäre versteht. Daran schliesst sich die dritte Generation datenschutzrechtlicher Regelungen an, die auch den Schutz von Daten, die nicht einer bestimmten identifizierbaren Person zugeordnet werden können, zum Gegenstand hat.

eigenverantwortliche Person, die nach freiem Willen Teil am politischen Willensbildungsprozess hat, wahrgenommen. Insofern ist Datenschutz auch eine Voraussetzung für die Wahrnehmung anderer Freiheiten.

Deutlich wird damit aber auch, dass im Schnittpunkt des Datenschutzrechts eine **Vielzahl von potenziell miteinander in Konflikt stehender Interessen** liegt, so dass ein Eingriff in das grundsätzlich bestehende alleinige Recht des Einzelnen, über die Verarbeitung ihn betreffender Daten zu entscheiden, durchaus möglich ist, wobei aber die einschlägigen völker- und verfassungsrechtlichen Vorgaben zu beachten sind. Dem **Verhältnismässigkeitsgrundsatz** und der **Abwägung der verschiedenen involvierten Interessen** untereinander kommt dabei eine herausragende Bedeutung zu, wobei immer der **„Kerngehalt" des Persönlichkeitsschutzes** zu beachten ist.[4]

III. Grundbegriffe des Datenschutzrechts – eine Auswahl

Das Datenschutzrecht beruht auf einer Reihe von Begriffen bzw. Begriffsdefinitionen, die einerseits seine Anwendbarkeit, andererseits die Tragweite verschiedener datenschutzrechtlicher Vorgaben determinieren. Im schweizerischen Recht werden diese Begriffe im Gesetz definiert, wobei einerseits auf das Bundesgesetz über den Datenschutz (DSG)[5], andererseits auf die kantonalen Datenschutzgesetze hinzuweisen ist, wobei in Bezug auf letztere im Folgenden – wie auch im weiteren Verlauf des Beitrags – beispielhaft auf das Freiburger Gesetz (DSchG)[6] zurückgegriffen wird.[7]

Nur am Rande sei in diesem Zusammenhang bemerkt, dass sich auch in der Gesetzgebung auf EU-Ebene, die für die Schweiz im Zuge des Inkrafttretens der „Bilateralen II" (insbesondere der Abkommen über „Schengen" und „Dublin") ebenfalls zu beachten ist,[8] entsprechende Definitionen finden, wobei teilweise (kleinere) Abweichungen zu verzeichnen sind, die jedoch allenfalls in Ausnahmefällen zu einer Unvereinbarkeit der schweizerischen Regelungen mit den Vorgaben des EU-Rechts führen dürften.[9]

Von besonderer Bedeutung sind in unserem Zusammenhang folgende Begriffe:

---

4 Vgl. ausführlich hierzu bereits ASTRID EPINEY, Zu ausgewählten Herausforderungen des Datenschutzrechts, in: Astrid Epiney/Sarah Theuerkauf (Hrsg.), Datenschtuz in Europa und die Schweiz, 2006, 1 (2 ff.).

5 SR 235.1.

6 Gesetz vom 25. November 1994 über den Datenschutz (DSchG), SR 17.1.

7 Zum jeweiligen Anwendungsbereich der Bundesgesetzgebung einerseits und der kantonalen Datenschutzgesetze andererseits noch unten IV.

8 Vgl. hierzu ausführlich ASTRID EPINEY, Datenschutz und „Bilaterale II", SJZ 2006, 121 ff.

9 Vgl. hierzu, in Bezug auf das DSG, EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, Schweizerisches Datenschutzrecht (Fn. 2), 276 ff. (insbesondere 279).

- **„Personendaten“** – nur bei ihrem Vorliegen kommen die datenschutzrechtlichen Regelungen zur Anwendung[10] – sind nach der Legaldefinition in Art. 3 lit. a DSG[11] alle „Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen“.

  Eine **Angabe** ist jede Art von Information, sei sie nun als Tatsachenfeststellung oder als Werturteil abgefasst, wobei sie aber in irgendeiner Form festgehalten sein muss, so dass reine „Gedankenspiele“ nicht erfasst werden. Auf die „Richtigkeit“ der Angaben kommt es nicht an.[12]
  Die Angabe muss einen **Bezug zu einer Person** aufweisen, was immer dann unproblematisch ist, wenn sich dieser Bezug aus der Natur der Information selbst ergibt, etwa die Krankengeschichte einer Person oder die Noten eines Schülers. Als solche nicht personenbezogene Informationen weisen gleichwohl einen Bezug zu einer Person auf, wenn sie aufgrund ihres Zusammenhangs oder sonstiger Informationen auch Rückschlüsse auf eine Person oder ihr Verhalten erlauben, wie etwa der Inhalt eines Protokolls einer Sitzung oder die Fotografie eines geparkten Autos. Fraglich könnte sein, ob Informationen, die als solche keinen Bezug zu einer Person aufweisen, wobei dieser aber möglicherweise hergestellt werden kann, einen Personenbezug aufweisen. Als Beispiel kann hier auf die Aufzeichnung der Internetzugriffe an einem öffentlichen Internetanschluss gedacht werden, die dann eine Zuordnung ermöglicht, wenn aufgrund anderer Elemente (Zeugenaussagen, Überwachungskameras o.ä.) festgestellt werden kann, wer zu welchem Zeitpunkt Zugriff auf den fraglichen Computer hatte. M.E. liegt hier ein potentieller Bezug zu einer Person vor, können die Informationen doch grundsätzlich einer Person zugeordnet werden, wobei zusätzlich auch die Bestimmbarkeit gegeben sein muss, so dass hier gewisse Querverbindungen des notwendigen Personenbezugs von Daten und der Bestimmbarkeit der Person bestehen.
  Bestimmbar ist eine Person, wenn die jeweilige Information zwar keinen eindeutigen Rückschluss auf die Identität zulässt (etwa durch Nennung des Namens und der Adresse oder durch eine einer Person zugewiesenen Nummer), sondern eine Identifikation aufgrund der gegebenen Informationen möglich ist (z.B.: ein 80-jähriger Patient des Pflegeheims in der Stadt X, der an Alzheimer erkrankt ist und Musiker war). Entscheidend ist, ob eine Identifizierung aufgrund der verfügbaren Informationen möglich ist und ob mit dieser nach den Umständen des Einzelfalls zu rechnen ist. Diese Voraussetzungen sind etwa im Falle des Vorgehens bei meldepflichtigen Erkrankungen gegeben, wenn auf einem Formular bei bestimmten Infektionskrankheiten vom behandelnden Arzt die Initialen aus Namen und Vornamen, Geschlecht, Geburtsdatum sowie Wohnort der infizierten Person gemeldet ist, ist hier doch eine Reindividualisierung in der Regel problemlos möglich und wohl auch wahrscheinlich, so dass hier gerade keine Anonymisierung – die sich begrifflich gerade dadurch auszeichnet, dass eine Identifizierung nicht (mehr) möglich ist – vorliegt. Bei pseudonymisierten Daten – also solchen, die mit einem irgendwie gearteten Schlüssel (dem Pseudonym) versehen sind, wobei eine Identifizierung jedoch möglich und häufig auch gewollt ist – handelt es sich zweifellos um Personendaten.[13]
  Keine Personendaten liegen vor, wenn es um Informationen über **Verstorbene** geht; einen postmortalen Persönlichkeitsschutz kennt das schweizerische Recht, abgesehen von eng begrenzten Ausnahmen, nicht.[14] Allerdings können sich die Angehörigen der verstorbenen Person auf ihren eigenen Persönlichkeitsschutz berufen, so dass Informationen über Verstorbene in der Regel als Personendaten der Angehörigen zu betrachten sind, da der Persönlichkeitsschutz einer Person auch den Schutz des Ansehens eines Verstorbenen oder das Recht auf Geheimhaltung bestimmter Angaben über diesen (wie etwa im Falle einer Krankheitsgeschichte) umfasst, sofern es sich um nahe Angehörige, in gewissen Fällen auch weiter entfernte Angehörige oder gar Freunde handelt, umfasst bzw. umfassen kann.[15]

- **„Besonders schützenswerte Personendaten“** sind nach Art. 3 lit. c DSG, Art. 3 lit. c DSchG Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche

---

10 Vgl. nur DAVID ROSENTHAL, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, 2008, Art. 3, Rn. 1.

11 Art. 3 lit. a) DSchG übernimmt diese Definition wörtlich.

12 Vgl. zum Ganzen ROSENTHAL, in: Handkommentar DSG (Fn. 10), Art. 3, Rn. 8 ff.

13 Vgl. zum Ganzen URS BELSER, in: Urs Maurer-Lambrou/Nedim Peter Vogt (Hrsg.), Datenschutzgesetz, 2. Aufl., 2006, Art. 3, Rn. 6.

14 Vgl. BELSER, in: DSG (Fn. 13), Art. 3, Rn. 9.

15 Vgl. aus der Rechtsprechung BGE 129 I 306 f.; BGE 127 I 145.

Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre oder Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe, sowie über administrative oder strafrechtliche Verfolgungen und Sanktionen. In Bezug auf diese, als besonders sensitiv eingeschätzte Daten kommen teilweise erhöhte Anforderungen in Bezug auf die Rechtmässigkeit der Bearbeitung zum Zuge.

Interessant ist in diesem Zusammenhang, dass in rechtsvergleichender Perspektive teilweise sehr unterschiedliche Daten als besonders sensibel angesehen werden. Im Übrigen ist darauf hinzuweisen, dass es für die Schutzwürdigkeit der fraglichen Personendaten nicht nur darauf ankommt, um welche Personendaten es sich handelt, sondern (auch) darauf, in welchem Zusammenhang sie bearbeitet werden bzw. wer von ihnen Kenntnis erlangt. So mag etwa die Information darüber, dass eine bestimmte Person den Fuss gebrochen hat,[16] im konkreten Fall erheblich weniger sensibel sein als eine Information über ihren Aufenthalt zu einem bestimmten Zeitpunkt an einem bestimmten Ort.

- Der Begriff des **Bearbeitens** umfasst nach Art. 3 lit. e DSG (sowie in ähnlicher Formulierung Art. 3 lit. d DSchG) jeden „Umgang mit Personendaten, ungeachtet der angewandten Mittel und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten". Damit werden letztlich „von der Wiege bis zur Bahre" alle Handlungen erfasst, die in irgendeiner Form Personendaten betreffen (können). Weiter wird sowohl die manuelle als auch die automatisierte Bearbeitung erfasst, so dass das Datenschutzrecht sowohl auf einzelne Blätter bzw. die darauf aufgezeichneten Informationen als auch auf grosse Datensammlungen Anwendung findet.[17] Kein Bearbeiten liegt allerdings vor, wenn es um einen lediglich gedanklichen Umgang mit Daten geht („die Gedanken sind frei", auch vom DSG); hingegen ist eine Bearbeitung unabhängig davon, ob sie mündlich oder schriftlich erfolgt. Irrelevant ist die subjektive Absicht des Datenbearbeiters für die Frage des Vorliegens einer Bearbeitung: So liegt im Falle der Beschlagnahmung des Mobiltelefons eines Schülers durch den Lehrer, damit ersterer dem Unterricht aufmerksam folgt, ein Beschaffen von Personendaten (nämlich derjenigen, die auf dem Mobiltelefon gespeichert sind) vor, auch wenn der Lehrer nicht die Absicht hat, etwa von den SMS Kenntnis zu nehmen.[18]

  In terminologischer Hinsicht ist darauf hinzuweisen, dass das europäische Unionsrecht in der Regel den Begriff der „Verarbeitung" verwendet, womit aber kein sachlicher Unterschied verbunden sein dürfte.

  Das in Art. 3 lit f DSG, Art. 3 lit. f DSchG erwähnte **Bekanntgeben** von Daten ist ein Unterfall der Bearbeitung, an den die Datenschutzgesetzgebung aufgrund der Sensitivität dieses Bearbeitungsvorgangs besondere Anforderungen stellt bzw. für den spezielle Bestimmungen gelten.[19] Eine Bekanntgabe im Sinne des Gesetzes liegt immer dann vor, wenn ein bestimmtes Verhalten zur Folge hat, dass Personen

---

16 Was seine Gesundheit betrifft und damit als besonders schützenswerte Angabe anzusehen ist, vgl. in Bezug auf das EU-Recht EuGH, Rs. C-101/01 (Lindqvist), Slg. 2003, I-12971.

17 Zu dieser weiten Fassung des Begriffs des Bearbeitens etwa ROSENTHAL, in: Handkommentar DSG (Fn. 10), Art. 3, Rn. 63 ff.

18 Vgl. das Beispiel bei ROSENTHAL, in: Handkommentar DSG (Fn. 10), Art. 3, Rn. 73.

19 Hierzu auch noch unten V.7.

Zugang zu Informationen erlangen, die ihnen vorher nicht bekannt waren;[20] dies kann durch aktives Handeln, aber auch durch Unterlassen (etwa das Nichtverschliessen eines Schrankes, in dem Personalakten aufbewahrt werden) geschehen. Eine Bekanntgabe kann auch zwischen Personen desselben Arbeitgebers stattfinden (etwa wenn eine Kommunikation zwischen Schul- und Sozialbehörde einer Gemeinde stattfindet).

IV. Zum anwendbaren Recht

Werden in Sozial- und Bildungsinstitutionen datenschutzrechtliche Fragen relevant, so fragt es sich zunächst, ob das Datenschutzgesetz des Bundes oder das jeweils einschlägige kantonale Datenschutzgesetz anwendbar ist (1.) sowie ob die Anwendung der Datenschutzgesetzgebung aus anderen Gründen ausgeschlossen ist (2.). Schliesslich ist noch auf die Bedeutung der Spezialgesetzgebung hinzuweisen (3.).

1. Zur Abgrenzung des Anwendungsbereichs des DSG und der kantonalen Datenschutzgesetze

Das Datenschutzgesetz des Bundes – das nach Art. 2 Abs. 1 DSG sowohl für natürliche als auch für juristische Personen gilt[21] – ist auf Datenbearbeitungen im privaten Bereich bzw. durch Privatpersonen und auf Datenbearbeitungen durch **Bundesorgane** anwendbar (Art. 2 Abs. 1 DSG). Unter den Begriff „Bundesorgane" fallen die Bundesverwaltung sowie Personen und Organisationen, die mit öffentlichen Aufgaben des Bundes betraut sind (Art. 3 lit. h DSG).
Die Datenbearbeitung durch **kantonale Behörden** hingegen wird durch die kantonale Datenschutzgesetzgebung geregelt. Entsprechend sind auch die (Aufsichts-) Kompetenzen der Datenschutzbehörden (EDÖB einerseits, kantonale Aufsichtsbehörden andererseits) ausgestaltet.

Die Datenbearbeitung durch **kantonale Behörden** fällt selbst dann nicht unter das DSG, wenn diese mit dem Vollzug von Bundesrecht betraut sind (Art. 2 Abs. 1 lit. b DSG, s. auch Art. 37 DSG). Dies erklärt sich durch die in der Bundesverfassung vorgesehene Kompetenzverteilung zwischen Bund und Kantonen, wonach eine Kompetenz des Bundes nur dann vorliegt, wenn diese ausdrücklich in der Verfassung vorgesehen ist. So kennt die Verfassung keine Bestimmung, die die Aufgabe des Datenschutzes explizit dem Bund zuweist und ihn zu einer umfassenden Regelung des Datenschutzes ermächtigt; gleichwohl kommen dem Bundesgesetzgeber auch in diesem Bereich gewisse Kompetenzen zu, denn er kann immer dann (auch) datenschutzrechtliche Fragen im Rahmen einer Annexkompetenz „mitregeln", wenn ihm für den betreffenden Bereich eine entsprechende Sachkompetenz zukommt. Insofern stützt sich der Bundesgesetzgeber zum Erlass von Datenschutzrecht auf Annexkompetenzen zu seinen Sachkompetenzen, wobei Art. 122 Abs. 1 BV (Zivilrecht), Art. 123 Abs. 1 BV (Strafrecht) sowie die entsprechenden Kompetenzen zum Erlass von Prozessrecht und Art. 164 Abs. 1 lit. g BV als Kompetenz, Organisation und Verfahren der Bundesbehörden zu regeln, von besonderer Bedeutung sind.

Das anwendbare Recht ist danach immer dann relativ problemlos zu bestimmen, wenn entweder Bundesbehörden oder kantonale Behörden handeln.

---

20 ROSENTHAL, in: Handkommentar DSG (Fn. 10), Art. 3, Rn. 76.

21 Wobei sich der folgende Beitrag auf die natürlichen Personen konzentriert.

Unter **Behörden und Dienststellen des Bundes** fallen alle Stellen der Bundesverwaltung (insbesondere Departemente, Bundesämter, Bundeskanzlei) sowie die eidgenössischen Anstalten (z.B. ETH, SUVA). Im Einzelnen sind hier das Regierungs- und Verwaltungsorganisationsgesetzt sowie die dazugehörige Verordnung[22] massgeblich.[23]

Abgrenzungsschwierigkeiten kann es in denjenigen Fällen geben, in denen **die Wahrnehmung bestimmter öffentlicher Aufgaben** auf **(öffentliche oder private) Institutionen übertragen** wird. Hier ist in aller Regel entscheidend, ob es sich um öffentliche Aufgaben des Bundes handelt, was die Anwendbarkeit des DSG insoweit nach sich zeiht, als sie Personendaten für die Erfüllung dieser öffentlichen Aufgabe des Bundes bearbeiten, oder ob es um öffentliche Aufgaben der Kantone geht (diesfalls sind die kantonalen Datenschutzgesetze anwendbar). Soweit erst gar keine Betrauung mit öffentlichen Aufgaben (des Bundes oder der Kantone) vorliegt oder die Datenbearbeitung nicht zur Wahrnehmung solcher öffentlichen Aufgaben erfolgt, sind die Vorgaben für die Datenverarbeitung durch Private (und damit das DSG mit der Aufsicht durch den EDÖB) heranzuziehen.
Diese Grundsätze können durch folgende Beispiele illustriert werden:[24]

- Als Bundesorgane sind die obligatorischen Unfallversicherer[25] sowie die vom Bund anerkannten Krankenversicherer anzusehen.
- Hingegen ist eine psychiatrische Klinik kein Bundesorgan im Sinne von Art. 2 Abs. 1 lit. a DSG, da die psychiatrische Versorgung der Bevölkerung eine kantonale Aufgabe ist, woran sich auch dann nichts ändert, wenn die Klinik auch im Rahmen eines fürsorgerischen Freiheitsentzugs (Art. 397a ff. ZGB) handelt.[26]
- Auch allgemein fällt das Gesundheitswesen, inkl. der Krankheitsbekämpfung, der Krankenbetreuung und der Vorsorge, in die Kompetenz der Kantone.
- Gleiches gilt selbstredend für die obligatorische und nachobligatorische Ausbildung (mit Ausnahme der Tätigkeiten der eidgenössischen Anstalten).
- Ganz allgemein reicht es für die Bejahung einer öffentlichen Aufgabe des Bundes nicht aus, dass der Bund bestimmte Tätigkeiten (mit-) finanziert. Ausschlaggebend ist vielmehr, wem (Bund oder Kantonen) die konkrete Organisation und Durchführung der Tätigkeiten obliegt. So ist etwa auch die Spitex – trotz der Bundessubventionierung – als öffentliche Aufgabe der Kantone anzusehen, da der Bund selbst in diesem Bereich gerade nicht tätig wird (und auch nicht tätig werden darf).[27]
- Ob und inwieweit eine Übertragung öffentlicher Aufgaben vorliegt, ist anhand der konkreten Umstände des Einzelfalls zu beurteilen. Entscheidend dürfte nicht nur sein,

---

22 RVOG und RVOV, SR : 172-010, SR 172.010.1.

23 Vgl. JÖHRI, in: Handkommentar DSG (Fn. 10), Art. 3, Rn. 99.

24 S. auch JÖHRI, in: Handkommentar DSG (Fn. 10), Art. 3, Rn. 100.

25 BGE 123 II 536, Erw. 1a, 3c.

26 BGE 122 I 153 Erw. 2c. S. auch Urt. des BG 1P.49/2007 v. 16.4.2007.

27 Gutachten Bundesamt für Justiz, VPB 70.54.

ob die betrauten Organisationen (anderen) Privaten aufgrund der einschlägigen gesetzlichen Regelung übergeordnet sind, sondern auch, ob aufgrund sonstiger Kriterien – z.B. die Finanzierung durch das Gemeinwesen, die Übertragung bestimmter Aufgaben durch Leistungsvereinbarung oder ein mehr oder weniger (sonstiger) direkter Einfluss des Staates auf die Aufgabenerfüllung – von einer Wahrnehmung öffentlicher Aufgaben auszugehen ist.[28] Jedenfalls die Trägerschaft der Organisation ist nicht ausschlaggebend. So sind etwa auch Privatkliniken, die auch – gestützt auf einen Vertrag mit den zuständigen kantonalen Behörden – sog. kantonale Patienten aufnehmen, insoweit dem kantonalen Datenschutzgesetz unterstellt.[29]

2. Zur Einschränkung des sachlichen Geltungsbereichs der Datenschutzgesetzgebung

Sowohl das Datenschutzgesetz des Bundes als auch diejenigen der Kantone sehen für bestimmte Datenkategorien und / oder Bearbeitungsvorgänge eine Einschränkung oder einen **Ausschluss der Anwendbarkeit der Datenschutzgesetzgebung** vor:

- So ist das Datenschutzgesetz des Bundes nicht anwendbar auf Daten, die ausschliesslich zum persönlichen Gebrauch verwendet werden, auf Datenverarbeitungen im Rahmen der politischen Beratungen auf Bundesebene, in hängigen Zivil- und Strafprozessen, der internationalen Rechtshilfe sowie in verwaltungsrechtlichen Verfahren ab der zweiten Instanz (Art. 2 Abs. 2 lit. a-c DSG). Ausserdem sind öffentliche Register des Privatrechts und Datenbearbeitungen durch das IKRK vom Datenschutzgesetz ausgenommen (Art. 2 Abs. 2 lit. d, e DSG) bzw. unterstehen speziellen Regelungen.
- Auf kantonaler Ebene sieht etwa das Freiburger Datenschutzgesetz vor, dass Verhandlungen der politischen Organe, hängige Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege sowie die im wirtschaftlichem Wettbewerb ausgeübten Tätigkeiten der öffentlichen Unternehmen (soweit diese nicht hoheitlich handeln) vom Anwendungsbereich des Gesetzes ausgeschlossen sind (Art. 2 Abs. 1 DSchG).

Von besonderer Bedeutung sind hier zweifellos die **hängige Verfahren** betreffenden Ausnahmen von der Eröffnung des Anwendungsbereichs der Datenschutzgesetzgebung. Ihr Hintergrund dürfte darin zu sehen sein, dass sich im Falle eines laufenden Verfahrens die Rechte der Beteiligten allein nach dem einschlägigen Verfahrensrecht bestimmen, das mit Rücksicht auf die besonderen Bedürfnisse des jeweiligen Verfahrens in Bezug auf den Umgang mit Personendaten spezielle Vorgaben kennt,[30] wobei schon aufgrund der erwähnten verfassungs- und europarechtlichen Vorgaben jedoch auch in diesem Rahmen dem

---

28 Gutachten Bundesamt für Justiz, VPB 70.54.

29 BGE 122 I 153 Erw. 2e, f.

30 Vgl. MAURER-LAMBROU/KUNZ, in: Datenschutzgesetz (Fn. 13), Art. 2, Rn. 27.

Persönlichkeitsschutz in angemessener Weise Rechnung zu tragen ist.[31] Allerdings kommt die Ausnahme nur während der Hängigkeit des Verfahrens zum Zuge, so dass Datenbearbeitungen vor und nach Beendigung eines Verfahrens dann wieder sehr wohl unter das Datenschutzgesetz fallen.

Die Frage der Hängigkeit ist nach den jeweils einschlägigen verfahrensrechtlichen Regeln zu beantworten, wobei grundsätzlich auch ausserordentliche Rechtsmittel zu berücksichtigen sind. Sobald aber eine Entscheidung oder eine Verfügung in Rechtskraft erwächst, ist das Verfahren jedenfalls als abgeschlossen zu betrachten.
Insofern begegnet ein Urteil des Freiburger Verwaltungsgerichts[32] Bedenken: Das Verwaltungsgericht wandte hier das Gesetz über die Verwaltungsrechtspflege[33] an, obwohl es sich sichtlich um einen abgeschlossenen Fall handelte. Konkret ging es um den Zugang von Eltern zu „persönlichen Notizen", die von der Präsidentin der Schulkommission im Zusammenhang mit der Frage der Einschulung eines Kindes in eine Regelklasse erstellt wurden und die von der Schulinspektorin dem Dossier des Kindes beigefügt wurden. Nachdem die Entscheidung über die Einschulung (entsprechend dem Wunsch der Eltern in einer Regelklasse) gefällt worden war, verlangten die Eltern Zugang zu den erwähnten Notizen. Das Verwaltungsgericht entschied den Fall allein auf der Grundlage des Gesetzes über die Verwaltungsrechtspflege, ohne das Verhältnis dieses Gesetzes zum Datenschutzgesetz auch nur zu problematisieren, dies obwohl es selbst feststellt, dass kein Verfahren in Bezug auf die Einschulung des Kindes mehr hängig war.

3. Zur Bedeutung der Spezialgesetzgebung

Datenschutz ist eine **„Querschnittsmaterie"**, so dass die jeweils geltenden und zu beachtenden Vorgaben häufig insofern vielschichtig sind, als viele, teilweise ineinander greifende Rechtsnormen zu beachten sind. Neben dem Datenschutzgesetz gibt es in den Spezialgesetzen – so auch in den gesetzlichen Grundlagen über Sozial- und Bildungsinstitutionen – spezifische Vorgaben (auch) über Fragen der Datenbearbeitung. Diese sind grundsätzlich neben den Vorgaben der (allgemeinen) Datenschutzgesetzgebung anzuwenden. Ein Zurücktreten der Datenschutzgesetzgebung – immer abgesehen von den bereits erwähnten Ausnahmen von ihrem Anwendungsbereich – kommt grundsätzlich nur dann in Frage, wenn die Spezialgesetzgebung strengere bzw. über die Datenschutzgesetzgebung hinausgehende oder diese präzisierende Vorgaben enthält.[34] Insofern sind die **allgemeinen, bereichsübergreifenden datenschutzrechtlichen Bestimmungen** grundsätzlich subsidiär heranzuziehen, und im Übrigen sind die allgemeinen verfassungs- und verwaltungsrechtlichen Grundsätze zu beachten, wozu – als Ausfluss des in Art. 13 BV grundrechtlich geschützten Rechts auf informationelle Selbstbestimmung – auch

---

31 Wobei die Anwendung des DSG aber nach dem klaren Wortlaut des Art. 2 Abs. 2 lit. c DSG auch dann ausgeschlossen ist, wenn das jeweils einschlägige Verfahrensrecht keinen dem DSG gleichwertigen Persönlichkeitsschutz garantiert (zumal diese Frage mitunter auch umstritten sein kann), vgl. ebenso ROSENTHAL/JÖHRI, in: Handkommentar DSG (Fn. 10), Rn. 30. A.A. MAURER-LAMBROU/KUNZ, in: Datenschutzgesetz (Fn. 13), Art. 2, Rn. 27.

32 Freiburger Zeitschrift für Rechtsprechung 2002, 427 ff., hierzu die Anmerkung von ASTRID EPINEY, Le champ d'application de la LPrD et le droit d'accès à des « notes personnelles » en matière scolaire, Revue fribourgeoise de Jurisprudence 2002, 434 ff.

33 RSF 150.1.

34 Vgl. insofern auch etwa BGE 128 II 311, 328 f.

grundsätzlich die datenschutzrechtlichen Bestimmungen gehören.[35] Darüber hinaus sind sie aber auch bei der Auslegung der jeweils zu beachtenden besonderen Vorgaben zu beachten. Insofern dürfte die effektive Beachtung datenschutzrechtlicher Vorgaben eine gewisse Vertrautheit nicht nur mit den jeweils für das entsprechende Sachgebiet heranzuziehenden Bestimmungen, sondern auch mit den allgemeinen Grundsätzen des Datenschutzrechts voraussetzen.

V. Datenschutzrechtliche Grundsätze und Rechte der Betroffenen

Das Datenschutzrecht beruht auf einer Reihe von **Grundsätzen**, die bereichsübergreifend in allen Konstellationen, in denen Daten bearbeitet werden, zu beachten sind. Sie finden sich im **Datenschutzgesetz des Bundes** im zweiten Abschnitt („Allgemeine Datenschutzbestimmungen", Art. 4 ff. DSG), sind aber auch – schon weil sie sich letztlich auch in den einschlägigen völker- und europarechtlichen Vorgaben finden – Teil der **kantonalen Datenschutzgesetze** (wenn auch die Formulierungen teilweise divergieren), so in Art. 4 ff. DSchG.

Diese Grundsätze geben die eigentlichen Leitideen des Datenschutzgesetzes wieder[36] und bilden daher letztlich die **Basis des Datenschutzrechts**. Es handelt sich hierbei um **Bearbeitungsgrundsätze**, die beim Bearbeiten von Personendaten eingehalten werden müssen. Als abstrakt-generelle Grundsätze müssen sie selbstredend auf die sich jeweils stellende Konstellation und den jeweiligen Sachbereich angewandt werden, so dass sie je nach dem betroffenen Bereich unterschiedliche Präzisierungen erfahren können.

Neben diesen Grundsätzen enthält das Datenschutzrecht noch eine **Reihe von Rechten Einzelner**, so insbesondere ein Auskunftsrecht (Art. 8 DSG, Art. 23 ff. DSchG) sowie die Rechte auf Berichtigung und auf Sperrung der Bekanntgabe (Art. 5 Abs. 2, 25 Abs. 3 lit. a, Art. 20, 25 DSG).

Weiter kennt das Datenschutzgesetz noch spezifische Anforderungen an die Datenbearbeitung durch öffentliche Organe sowie durch Private.

Im Folgenden sollen die wichtigsten datenschutzrechtlichen Grundsätze und Rechte der Einzelnen erörtert werden, dies unter Berücksichtigung der Rechtsprechung des Bundesgerichts und der kantonalen Gerichte, aber auch unter Heranziehung m.E. möglicher typischer Problemstellungen (wobei der Akzent auf Problemstellungen aus dem Bereich der Sozial- und Bildungsinstitutionen liegt). Dabei sollen einerseits die allgemeinen datenschutzrechtlichen Grundsätze, andererseits aber auch die spezifisch für öffentliche Organe zum Zuge kommenden Anforderungen berücksichtigt werden, während die für Datenbearbeitungen Privater zur Anwendung kommenden Vorgaben nicht behandelt werden.

---

35 BVGE 2009/24, C-6570/2007, Urt. v. 29.5.2009, Erw. 4.

36 BBl 1988 II 449.

Im Einzelnen soll auf folgende Problemkreise eingegangen werden: Grundsatz der Rechtmässigkeit und Erfordernis einer gesetzlichen Grundlage (1.), Grundsatz von Treu und Glauben (2.), Verhältnismässigkeitsprinzip (3.), Zweckbindungsgrundsatz (4.), einige weitere allgemeine datenschutzrechtliche Grundsätze (5.), für gewisse besondere Formen der Datenbearbeitung (Beschaffen von Personendaten und Datenbekanntgabe) geltenden spezifischen Vorgaben (6., 7.) sowie Auskunfts- bzw. Einsichtsrecht (8.).

1. Grundsatz der Rechtmässigkeit und Erfordernis einer gesetzlichen Grundlage

Nach Art. 4 Abs. 1 DSG dürfen Personendaten nur **rechtmässig bearbeitet** werden. Ein rechtswidriges Verhalten liegt dabei immer schon dann vor, wenn die Bearbeitung der Daten[37] gegen eine in der Schweiz geltende rechtlich verbindliche Norm verstösst. Die Verletzung der in der Schweiz geltenden Rechtsordnung bei der Beschaffung und weiteren Bearbeitung von Personendaten ist damit allgemein unzulässig.

Bundesbehörden und kantonale Behörden dürfen als Ausfluss bzw. Präzisierung des Rechtmässigkeitsprinzips nur dann Datenbearbeitungen vornehmen, wenn hierfür eine **gesetzliche Grundlage** existiert. M.a.W. genügt es für die Rechtmässigkeit einer solchen Bearbeitung gerade nicht, dass ihr keine Rechtsnormen entgegenstehen, sondern die **Bearbeitung muss vielmehr ausdrücklich in einem Gesetz** vorgesehen sein.

Für **Bundesorgane** ist **Art. 17 DSG** von besonderer **Bedeutung**. Danach dürfen Bundesorgane Personendaten grundsätzlich (zu den Ausnahmen Art. 19, 22 DSG) bearbeiten, wenn sich die Bearbeitung auf eine genügende gesetzliche Grundlage stützt. Zudem ist spezifisch bei der Beschaffung noch Art. 18 DSG zu beachten.[38]

Entsprechend sieht **Art. 4 DSchG** vor, dass eine Datenbearbeitung durch ein öffentliches Organ nur dann zulässig ist, wenn eine gesetzliche Bestimmung diese Bearbeitung vorsieht oder (im Falle des Fehlens einer solchen gesetzlichen Grundlage) die Bestimmungen über die Erfüllung seiner Aufgaben es voraussetzen. Da die zuletzt genannte Alternative letztlich eine Ausnahme von dem Grundsatz der gesetzlichen Grundlage darstellt, ist sie restriktiv auszulegen, so dass eine Datenbearbeitung auf der Grundlage dieser Bestimmung nur dann zulässig ist, wenn sie in dem entsprechenden Umfang zwingend für die Erfüllung der öffentlichen Aufgabe notwendig sind. Jedenfalls sind ggf. bestehende zusätzliche Vorgaben für bestimmte Formen des Bearbeitens (Art. 9 ff. DSchG) zu beachten. Es ist in diesem Zusammenhang bemerkenswert, dass die entsprechende Bestimmung des DSG keine solche „Verwässerung" des Grundsatzes der Erforderlichkeit einer gesetzlichen Grundlage kennt.

Unter **gesetzlicher Grundlage** ist ein **Gesetz im materiellen Sinn** zu verstehen, so dass die Bearbeitung von Personendaten in einer generell-abstrakten Norm vorgesehen sein muss. Bei der gesetzlichen Grundlage kann es sich um eine Verfassungs- oder Gesetzesbestimmung, um eine gestützt darauf erlassene Verordnungsnorm oder einen völkerrechtlichen Vertrag handeln.[39] Eine gesetzliche Grundlage ist also nicht nur ein **Gesetz im formellen Sinn**, wie dies in Art. 17 Abs. 2 DSG für die besonders schützenswerten Personendaten verlangt wird.

Sofern es um einen **schweren Eingriff in die Persönlichkeitsrechte** oder die Privatsphäre durch die Datenbearbeitung geht, muss jedoch – unabhängig von der Frage, ob es um die Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen geht – ein **Gesetz im formellen Sinn** vorliegen, wie sich aus **Art. 36 Abs. 1 S. 2 BV** ergibt, wonach „schwerwiegende Einschränkungen" von Grundrechten im Gesetz selbst vorgesehen sein müssen. Diese Voraussetzung kann etwa dann gegeben sein, wenn nicht die Art der Daten, sondern die Form ihrer Beschaffung einen besonders schweren Eingriff in die Persönlichkeitsrechte darstellt (z.B. im Falle geheimer Überwachung).

---

37 Zum weiten Begriff der Datenbearbeitung bereits oben III.

38 Zur Beschaffung von Daten auch noch unten V.6.

39 BBl 1988 II 467.

Damit die somit jedenfalls erforderliche **gesetzliche Grundlage als genügend** erachtet werden kann, muss sie mindestens den Zweck, die beteiligten Bundesorgane sowie das Ausmass der Datenbearbeitung in den Grundzügen festlegen. Eine gesetzliche Grundlage für Bundesorgane ist unter folgenden Voraussetzungen **hinreichend bestimmt**:[40]

- Definition des Bearbeitungszwecks;
- Umschreibung des Umfangs der Datenbearbeitung in groben Zügen;
- Festhalten der an der Datenbearbeitung Beteiligten sowie
- Aufführen der Kategorien der bearbeiteten Daten bei besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen.

Allerdings hängt der im **Einzelnen zu fordernde Grad der Bestimmtheit** von den **Umständen des Einzelfalls** und damit verschiedenen Kriterien ab, so insbesondere der Schwere des Eingriffs in die Persönlichkeitsrechte, der Art der bearbeiteten Daten, der Kreis der betroffenen Personen sowie der Komplexität der zu treffenden Entscheidung.[41]

Deutlich wird damit, dass sich die Rechtmässigkeit der Datenbearbeitung durch kantonale Behörden oder Bundesbehörden regelmässig nur auf der Grundlage der genauen Analyse der Tragweite der jeweils einschlägigen Spezialgesetzgebung ermitteln lässt.[42]

Im Falle des Fehlens einer gesetzlichen Grundlage für die zur Debatte stehende Datenbearbeitung durch ein öffentliches Organ ist diese grundsätzlich rechtswidrig, wobei die in der Datenschutzgesetzgebung selbst vorgesehenen Ausnahmen vorbehalten bleiben.[43]

Daher waren – vor der Schaffung einer gesetzlichen Grundlage – die Pläne der EDK (Konferenz der kantonalen Erziehungsdirektoren), Lehrer, die eines Sexualvergehens gegen Kinder oder des Herunterladens kinderpornographischer Seiten auf dem Internet oder ähnlicher Delikte verdächtigt oder wegen eines entsprechenden Delikts verurteilt worden waren, in einer bei der EDK geführten Datenbank zu speichern mit dem Ziel, die Einstellung eines wegen eines solchen Delikts bzw. eines entsprechenden Verdachts freigestellten oder entlassenen Lehrers in einem anderen Kanton zu verhindern, rechtswidrig. Hieran ändert auch der Umstand nichts, dass das Anliegen der EDK zweifellos berechtigt war.
Ebenso dürfen z.B. Informationen über das Verhalten von Schülern (in oder ausserhalb der Schule) ohne eine gesetzliche Grundlage nicht erhoben und bearbeitet werden. Daher ist etwa das Anlegen eines „Schülerdossiers", das von Schule zu Schule weitergegeben wird und über das „normale" Zeugnis hinausgehende Informationen enthält, die ausserhalb eines Verfahrens „gesammelt" wurden, ohne gesetzliche Grundlage rechtswidrig.
Ebensowenig stellen die allgemeinen staatlichen Aufsichtspflichten im Schulbereich eine ausreichende Rechtsgrundlage dar, um die Vereinszugehörigkeit bestimmter Lehrpersonen zu erfassen.[44]

2. Grundsatz von Treu und Glauben

Der in Art. 4 Abs. 2 DSG und Art. 5 Abs. 1 DschG verankerte **Grundsatz von Treu und Glauben** besagt allgemein, dass ein **loyales und vertrauenswürdiges Verhalten im**

---

40 Vgl. EDÖB, 11. Tätigkeitsbericht, 13.

41 BBl 1988 II 467.

42 Vgl. zur Bedeutung der Spezialgesetzgebung bereits oben IV.3.

43 Vgl. etwa in Bezug auf die Bekanntgabe unten V.7.

44 BGE 122 I 360.

Rechtsverkehr grundlegend ist, dem widersprüchliches Verhalten zuwider läuft.[45] Er ist insbesondere insofern von Bedeutung, als er eine **Generalklausel** darstellt und in all denjenigen Konstellationen zum Zuge kommt bzw. kommen kann, in denen die **anderen Bearbeitungsgrundsätze nicht greifen**.[46]

Angesichts des Umstandes, dass sich weder aus dem DSG noch aus den (zumindest meisten) kantonalen Datenschutzgesetzen eine allgemeine Pflicht ableiten lässt, Personen, deren Daten bearbeitet werden, in jedem Fall aktiv zu informieren, kommt dem Grundsatz von Treu und Glauben gerade in diesem Bereich eine wichtige Bedeutung zu: Ihm dürfte eine allgemeine Verpflichtung dergestalt zu entnehmen sein, dass die Betroffenen immer dann über die **Bearbeitung ihrer Daten zu informieren** sind, wenn sich dies angesichts der Umstände unter Zugrundelegung eines loyalen und vertrauenswürdigen Verhaltens aufdrängt.
Ebenfalls aus dem Grundsatz von Treu und Glauben ableitbar ist die grundsätzliche Pflicht der Datenbeschaffung direkt bei dem Betroffenen, nicht hingegen bei Dritten, wobei dies teilweise auch (vgl. Art. 9 Abs. 1 DschG) in kantonalen Datenschutzgesetzen verankert ist.

3. Grundsatz der Verhältnismässigkeit

Allgemein besagt der bereits in der Bundesverfassung sowie in Art. 4 Abs. 2 DSG, Art. 6 DSchG figurierende Grundsatz der Verhältnismässigkeit, dass eine staatliche Massnahme **geeignet und erforderlich** (also das mildeste Mittel) sein muss, um den mit dem öffentlichen Interesse verfolgten Zweck herbeizuführen und dass eine **Abwägung von öffentlichen Interessen und betroffenen privaten Interessen** (Verhältnismässigkeit i.e.S.) vorzunehmen ist.

Der Grundsatz der Verhältnismässigkeit ist insbesondere dann von besonderer Bedeutung, wenn eine gesetzliche Grundlage für die Datenbearbeitung sehr allgemein gehalten ist. Denn auch wenn eine solche Rechtsgrundlage einschlägig ist, darf eine Datenbearbeitung nicht ohne Einhaltung des Verhältnismässigkeitsprinzips vorgenommen werden. Mit anderen Worten ist die Geeignetheit, die Erforderlichkeit sowie die Verhältnismässigkeit i.e.S. (so dass die Datenbearbeitung auch unter Abwägung der in Frage stehenden Interessen zumutbar sein muss) einer Datenbearbeitung jeweils im Einzelnen zu hinterfragen und zu prüfen: Die Bearbeitungsgrundsätze müssen grundsätzlich in Bezug auf den Zweck sowie auf die Art der Bearbeitung erfüllt sein. Dies bedingt, dass Daten von Vornherein nur dann bearbeitet werden dürfen, wenn sie für einen bestimmten Zweck objektiv geeignet und tatsächlich erforderlich sind.[47]
Ob der Grundsatz der Verhältnismässigkeit eingehalten wird, kann nicht generell beantwortet werden, sondern ist in jedem **Einzelfall** zu überprüfen. Eine solche einzelfallabhängige Abklärung der Einhaltung der Anforderungen des Verhältnismässigkeitsgrundsatzes muss nach objektiven Kriterien vorgenommen werden, d.h. dass nicht auf die subjektive Sichtweise jeder einzelnen Person abzustellen ist, wobei jedoch die Bildung von Personen- bzw. Datenkategorien möglich ist.[48]
Jedenfalls impliziert die Heranziehung des Grundsatzes der Verhältnismässigkeit, dass in einem ersten Schritt der mit der entsprechenden **Datenbearbeitung verfolgte Zweck** eruiert wird, handelt es sich doch bei der Verhältnismässigkeit um eine **Mittel-Zweck-Relation**, so dass die Verhältnismässigkeit der herangezogenen Mittel nur in Bezug auf einen definierten Zweck eruiert werden kann.

Fall 1 (BGE 133 V 359):
Eine Krankenversicherung (Helsana) verlangt von bestimmten Leistungserbringern (im konkreten Fall von Pflegeheimen) die Herausgabe von Unterlagen, welche die Grundlage für die Pflegebedarfseinstufung bilden,

---

45 YVO HANGARTNER, in: Bernhard Ehrenzeller/Philippe Mastronardi/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.), Die schweizerische Bundesverfassung, Kommentar, 2. Aufl., 2 Bde, 2008, Art. 5 BV, Rn. 43.

46 ROSENTHAL, in: Handkommentar (Fn. 10), Art. 4 Rn. 14.

47 BBl 1988 II 450.

48 Vgl. ROSENTHAL, Handkommentar (Fn. 10), Art. 4, Rn. 22 f.

was auf den Pflegebericht und die Vitalzeichenkontrolle zutrifft. Diese Herausgabe wurde von dem Pflegeheim verweigert, das nur dann zur Herausgabe bereit war, wenn der Versicherer das Gesuch im Einzelfall konkret begründet sowie belegen kann, dass er die entsprechenden Angaben zur Erfüllung seiner Aufgaben benötigt.
Das Bundesgericht hielt fest, dass die zu Lasten der obligatorischen Krankenpflegeversicherung erbrachten Leistungen wirksam, zweckmässig und wirtschaftlich sein müssten, wobei der Krankenversicherer berechtigt und verpflichtet sei zu überprüfen, ob die erbrachten Leistungen das Wirtschaftlichkeitsgebot respektieren; für nicht wirtschaftliche Leistungen könne denn auch nach Art. 56 Abs. 2 S. 1 KVG die Vergütung verweigert werden. Der Versicherer müsse daher auch die Einstufung der Pflegebedürftigkeit prüfen, sei eine zu hohe Einstufung doch eine nicht wirtschaftliche Leistung, die verweigert werden müsse.
Nach Art. 84, 84a KVG seien die Krankenversicherer befugt, die Personendaten, einschliesslich besonders schützenswerter Personendaten und Persönlichkeitsprofile, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach dem KVG übertragenen Aufgaben zu erfüllen, namentlich unter anderem um Leistungsansprüche zu beurteilen. Die spezielle Bestimmung des Art. 42 halte zudem fest, dass der Leistungserbringer dem Versicherer eine detaillierte und verständliche Rechnung zustellen muss und ihm auch alle Angaben machen muss, die notwendig sind, um die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung überprüfen zu können. Nach Art. 42 Abs. 4 KVG könne der Versicherer eine genaue Diagnose oder zusätzliche Auskünfte medizinischer Natur verlangen. Diese Bestimmungen stellten eine formellgesetzliche Grundlage im Sinne des Art. 17 Abs. 2 DSG dar. Der Umfang der in diesen Bestimmungen verankerten Auskunftspflicht richte sich danach, was der Versicherer für die Durchsetzung seiner Rechte und der Pflicht zur Kontrolle der Wirtschaftlichkeit als notwendig erachtet. Dabei sei allerdings das Verhältnismässigkeitsprinzip zu beachten, in dessen Rahmen jedoch dem Versicherer ein gewisser Beurteilungsspielraum eingeräumt werden müsse, auf welche Weise und mit welchen Angaben er die Überprüfung der Wirtschaftlichkeit vornimmt. Unterlagen, die über den gesundheitlichen Zustand des Patienten Aufschluss geben, seien grundsätzlich geeignet und erforderlich für die Überprüfung der Richtigkeit der Pflegebedarfsermittlung und damit die Wirtschaftlichkeitskontrolle, so dass die Herausgabe solcher Daten grundsätzlich vom Leistungserbringer verlangt werden könne.
Eine solche Herausgabe könne auch generell verlangt werden und bedürfe nicht eines im Einzelfall begründeten Gesuchs. Denn ein solches Erfordernis ergebe sich nicht aus den genannten gesetzlichen Grundlagen. Und wenn die Herausgabe solcher Berichte generell geeignet und erforderlich für die Prüfung der Pflegebedarfseinstufung sind, treffe dies auch auf jeden einzelnen Fall zu. Im Übrigen sei es angesichts der grossen Menge von Abrechnungen nicht möglich, von den Versicherern zu verlangen darzulegen, warum sie bei einer bestimmten Person eine Überprüfung vornehmen wollen; vielmehr müsse es zulässig sein, dass die Versicherer lediglich Stichproben vornehmen, für die jedoch eine generelle Übermittlung der erforderlichen Daten notwendig sei.
Damit wird den Krankenversicherern ein denkbar weiter Gestaltungsspielraum eingeräumt, und die Erforderlichkeit der Übermittlung der verlangten, zudem sensiblen Daten letztlich nicht geprüft. Die generalisierte Übermittlung der hier zur Debatte stehenden Daten läuft letztlich auf eine Art „Datensammlung auf Vorrat“ hinaus, die grundsätzlich nicht mit dem Verhältnismässigkeitsgrundsatz in Einklang steht.[49] Zwar ist zuzugeben, dass eine Begründung im Einzelfall möglicherweise aufwendiger sein könnte; es ist aber – entgegen der Ansicht des Bundesgerichts – sehr zu bezweifeln, ob dieser Aspekt wirklich derart ins Gewicht fällt, zumal man ihm ja auch bei den Anforderungen an die Begründung des Einzelfalls hätte Rechnung tragen können. Dass aber solche Erwägungen tragend sind für die Zulässigkeit einer generalisierten Übermittlung sensibler Daten, dürfte kaum den im Datenschutzgesetz zum Ausdruck gekommenen und auch im Rahmen der Auslegung des KVG zu beachtenden Wertung entsprechen. Schliesslich überrascht, dass das Bundesgericht nicht prüfte, ob eine anonymisierte Weitergabe der Daten nicht den Anforderungen der Verhältnismässigkeit besser entsprochen hätte.
Nur am Rande sei in diesem Zusammenhang bemerkt, dass der Hinweis des Bundesgerichts am Schluss des Urteils, schliesslich unterständen ja die Krankenversicherer einer Schweigepflicht und dem Arztgeheimnis, eigentlich nichts zur Sache tut, da diese Erwägung nicht die Unverhältnismässigkeit einer Datenbearbeitung zu rechtfertigen vermag. Insbesondere kann aus diesen Pflichten sicherlich nicht abgeleitet werden, dass damit alle einer solchen Schweigepflicht unterstehenden Personen Zugang zu allen Daten haben dürfen (etwa alle Angestellten einer Versicherung zu allen medizinischen Dossiers).[50]

Fall 2 (BVGE 2009/24, C-6570/2007, Urt. v. 29.5.2009):

---

49 Möglicherweise könnte man das Urteil des Bundesgerichts auch so auslegen, dass nur die für die Durchführung der Stichproben erforderlichen Daten verlangt werden können, allerdings wird eine solche Auslegung (die grundsätzlich begrüssenswert ist) nicht durch den Wortlaut des Urteils gestützt.

50 Vgl. zu dieser Problematik im Zusammenhang mit dem Fall CSS URSULA UTTINGER, Datenschutz in der Krankenversicherung, insbesondere im vertrauensärztlichen Dienst, HAVE 2007, 253 ff.

In diesem, teilweise dem Fall 1 ähnlich gelagerten Fall, stand zur Debatte, ob bei Eintritt von Akutpatienten zur stationären Behandlung in öffentliche Spitäler in einem Mustervertrag vorgesehen werden darf, dass nicht nur der Behandlungsgrund (Krankheit, Unfall, Mutterschaft) bzw. eine allgemeine Eingriffsindikation, sondern auch die Diagnose sowie der sog. Eingriffscode gemäss Art. 42 Abs. 4 KVG an die Krankenversicherer weiterzugeben sind.
Das Bundesverwaltungsgericht bejahte die Existenz einer formell-gesetzlichen Grundlage (Art. 84 lit. c KVG, Art. 84a Abs. 1 lit. a, Art. 42 Abs. 4 KVG) und die grundsätzliche Zulässigkeit einer systematischen Weitergabe auch von Diagnosen durch den Leistungserbringer an die Versicherer. Ein solches Vorgehen entspreche grundsätzlich auch den Anforderungen der Verhältnismässigkeit. Jedoch könne aus dem Verhältnismässigkeitsgrundsatz auch abgeleitet werden, dass die genaue Ausgestaltung dieser Weiterleitung (Modalitäten der Weitergabe, z.B. an den Vertrauensarzt, Dauer der Aufbewahrung, Weitergabe nur in dem unbedingt erforderlichen Detaillierungsgrad) zu präzisieren sei.
Letztlich schränkt dieses Urteil die in BGE 133 V 359 grundsätzlich angenommene Pflicht zur systematischen Herausgabe medizinischer Diagnosen an die Versicherer doch in wesentlichen Punkten ein, wenn auch das Bundesverwaltungsgericht (verständlicherweise) nicht an den bereits bedenklichen Grundannahmen des Bundesgerichts rüttelt. Jedenfalls ist aber genau darauf zu achten, dass die weitergegebenen Daten tatsächlich einen Zusammenhang mit der Wirtschaftlichkeitskontrolle aufweisen, was wohl nicht auf alle Diagnosedaten zutrifft (z.B. solche über das Suchtverhalten einer Person oder seines sozialen Umfelds).
Nur am Rande sei in diesem Zusammenhang bemerkt, dass eine systematische Weitergabe von Diagnosen an Krankenversicherer nicht nur aus Gründen des Persönlichkeitsschutzes i.e.S. bedenklich ist, sondern auch vor dem Hintergrund der sehr weit gespannten Aktivitäten der Krankenversicherer zu würdigen ist: Diese bieten nämlich in aller Regel nicht nur die obligatorische Grundversicherung, sondern auch Zusatzversicherungen an, wobei es bei den Verhandlungen mit den Versicherten über die hier zu zahlenden Prämien durchaus interessant sein kann zu wissen, welche medizinischen Diagnosen in Bezug auf eine bestimmte Person in der Vergangenheit gestellt wurden. Eine derartige Verwendung dieser Daten verstiesse zwar klar gegen den Zweckbindungsgrundsatz; sind Daten aber einmal vorhanden, so ist ihre nicht ganz zweckkonforme Nutzung nie wirklich auszuschliessen, übrigens auch ein Grund dafür, dass Daten wirklich immer nur im notwendigen Mass bearbeitet werden sollen.

4. Grundsatz der Zweckbindung

Nach **Art. 4 Abs. 3 DSG** (s. auch Art. 5 DSchG) dürfen Personendaten nur zu dem Zweck bearbeitet werden, der **bei der Beschaffung angegeben** wurde, aus den **Umständen ersichtlich** oder **gesetzlich vorgesehen** ist. Durch diesen so umschriebenen Grundsatz der Zweckbindung soll erreicht werden, dass den von einer Datenbearbeitung betroffenen Personen bereits zu Beginn deutlich wird, wofür ihre Daten verwendet werden und dass die Daten nicht „zweckentfremdet“ werden.

Interessant ist die Aufweichung der Zweckbindung in Art. 5 Abs. 1 DSchG, der vorsieht, dass die Personendaten auch zu einem anderen Zweck als derjenige, für den sie beschafft wurden, bearbeitet werden können, soweit dieser mit dem ursprünglichen Zweck nach Treu und Glauben vereinbar ist, eine Frage, die mitunter schwierig zu beantworten sein kann.

Für die öffentliche Verwaltung ist das Zweckbindungsprinzip in aller Regel im Zusammenhang mit der gesetzlichen Grundlage von Bedeutung, die den Zweck grundsätzlich abschliessend umschreiben muss.

5. Weitere allgemeine datenschutzrechtliche Grundsätze

Darüber hinaus sei noch auf einige weitere bedeutende datenschutzrechtliche Grundsätze hingewiesen:

- **Grundsatz der Transparenz** (Art. 4 Abs. 4 DSG, Art. 9 Abs. 2 DSchG): Die **Beschaffung von Personendaten**, sowie ggf. der Zweck ihrer Bearbeitung, muss für die betroffene Person **erkennbar** sein. Damit soll insbesondere eine transparente Datenbeschaffung für die betroffenen Personen sichergestellt werden.[51]

  Bemerkenswert ist, dass sich diese Erkennbarkeit nur auf die Beschaffung, nicht hingegen (wie bei den anderen Grundsätzen) auf die Bearbeitung als solche bezieht. Allerdings kann sich aus anderen Grundsätzen, insbesondere dem Grundsatz von Treu und Glauben, eine Informationspflicht der betroffenen Personen auch über die Bearbeitung ergeben

  Öffentliche Organe dürfen Personendaten grundsätzlich nur aufgrund einer gesetzlichen Grundlage bearbeiten und somit beschaffen, wobei sich die Erkennbarkeit im Falle der Beschaffung bei Dritten in der Regel bereits aus der gesetzlichen Grundlage ergeben wird.

  Ausnahmsweise kann aber das Beschaffen auch **ohne das Wissen der betroffenen Person** stattfinden, wenn hierfür eine **gesetzliche Grundlage** besteht. Dies ist insbesondere im Bereich der Polizei und der Strafverfolgung der Fall
- **Grundsatz der Datenrichtigkeit und der Datensicherheit** (Art. 5 Abs. 1, 7 DSG, Art. 7 DSchG): Nach dem Grundsatz der Datenrichtigkeit hat sich der Datenbearbeiter der Richtigkeit der bearbeiteten Daten zu vergewissern, und unvollständige oder unrichtige Daten sind zu berichtigen oder zu vernichten. Die Datensicherheit verlangt angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten.
- **Datenschutzrechtliche Verantwortung**: Das zuständige Bundesorgan bzw. das zuständige kantonale Organ ist umfassend für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich. Dieser Grundsatz gilt auch, wenn das öffentliche Organ Dritte als Hilfspersonen beizieht oder die Datenbearbeitung vollständig ausgelagert wird (Art. 10a, 16 DSG, Art. 17, 18 DSchG). Die Rechtsposition des Betroffenen darf sich also durch die Auslagerung einer Datenbearbeitung in keiner Weise verschlechtern.

  Die einschlägigen gesetzlichen Vorgaben erlauben also grundsätzlich ein **Outsourcing**, es sei denn, dem stünden gesetzliche oder vertragliche Geheimhaltungspflichten entgegen, wie z.B. beim Bankgeheimnis. Allerdings muss das beauftragende öffentliche Organ dafür sorgen, dass die **Datenbearbeitung allen einschlägigen gesetzlichen Vorgaben genügt**, die es auch selbst zu beachten hätte. Insbesondere muss sich der Auftraggeber vergewissern, dass die Anforderungen an die Datensicherheit eingehalten werden, so dass die notwendigen technischen und organisatorischen Massnahmen ergriffen werden, damit die Personendaten vor jeder unbefugten Bearbeitung geschützt werden. Dem **Auftraggeber** obliegt hier also eine **umfassende Sorgfaltspflicht**.
  Damit tatsächlich die Einhaltung dieser Vorgaben sichergestellt sein kann, ist in der Regel der Abschluss eines entsprechenden **Vertrages** notwendig, in dem der Auftragnehmer die einschlägigen Verpflichtungen eingeht.[52] In einer solchen Vereinbarung sind in der Regel etwa folgende Aspekte zu berücksichtigen:
  - genauer Umfang der Datenbearbeitung durch den Auftragnehmer bzw. genaue Bezeichnung der Dienstleistung;
  - Zugriff auf die Daten;

---

51 BBl 2003 2124.

52 Vgl. in diesem Zusammenhang auch die Checklisten für das Outsourcing auf www.dsb.zh.ch/themen.php?action=list&themesid=212&zoom_query=Outsourcing.

- Fragen der Bekanntgabe;
- verwendete Technologie, Datensicherheit und Sicherheitskonzept;
- Archivierung;
- Geheimhaltungspflichten;
- Kontrolle der Einhaltung der Vorgaben und ggf. Berichts- und Informationspflichten.

Trifft das **öffentliche Organ nicht die sich nach den Umständen aufdrängenden Vorkehrungen**, damit der Auftragnehmer die einschlägigen gesetzlichen Verpflichtungen auch tatsächlich einhält, liegt eine **Persönlichkeitsverletzung durch das betreffende Organ** vor. Denn diesfalls geht es um eine Bekanntgabe von Personendaten ohne Beachtung der hierfür einschlägigen rechtlichen Voraussetzungen. Fraglich ist, ob die Verantwortlichkeit des Bundes oder des jeweiligen Kantons auch dann begründet wird, wenn die zuständigen Organe zwar alle notwendigen Massnahmen ergriffen haben, der Auftragnehmer aber gleichwohl gegen eine der einschlägigen gesetzlichen Vorgaben verstösst. Nach der hier vertretenen Ansicht ist auch in einem solchen Fall die Verantwortlichkeit des Bundesorgans zu bejahen, denn letztlich muss es ihm zugerechnet werden, wenn der Auftragnehmer sich nicht an die gesetzlichen Vorgaben hält. Insofern kann man durchaus von einer „Erfolgspflicht" sprechen.

6. Insbesondere: zum Beschaffen von Personendaten

Für das **Beschaffen von Personendaten** – eine besondere Form der Bearbeitung[53] – bestehen auf Bundesebene und (zumindest teilweise) auf kantonaler Ebene über die allgemeinen Grundsätze hinaus noch **besondere Vorgaben**.

- Auf **Bundesebene** ist auch im Falle der Datenbeschaffung bei einer anderen Verwaltungsstelle eine entsprechende **gesetzliche Grundlage** notwendig. Ausnahmen sind grundsätzlich (abgesehen von spezialgesetzlichen Bestimmungen) nur unter den Voraussetzungen des **Art. 19 Abs. 1 lit. a, b, c DSG** (betreffend die Bekanntgabe von Personendaten) zulässig. Darüber hinaus enthalten Art. 18 DSG und Art. 24 VDSG weitere Vorgaben über die Information der Betroffenen beim Beschaffen von Personendaten im Falle der systematischen Erhebung von Daten oder der Beschaffung besonders schützenswerter Daten oder von Persönlichkeitsprofilen.
- Auf **kantonaler Ebene** enthält z.B. Art. 9 Abs. 2, 3 DSchG ähnliche Informationspflichten. Darüber hinaus sieht Art. 9 Abs. 1 S. 1 DschG das sich schon aus dem Grundsatz von Treu und Glauben ergebende Prinzip vor, dass Personendaten grundsätzlich bei der betroffenen Person zu erheben sind. Allerdings dürfen sie dann bei einem öffentlichen Organ oder einem Dritten eingeholt werden, wenn eine gesetzliche Bestimmung es vorsieht, die Natur der Aufgabe es erfordert oder wenn besondere Umstände es rechtfertigen (Art. 9 Abs. 1 S. 2 DSchG). Diese eher unbestimmt gefasste Ausnahmebestimmung sollte grundsätzlich restriktiv ausgelegt werden, so dass etwa „besondere Umstände" wohl nur im Einzelfall vorliegen dürften und jedenfalls keine systematische Datenbeschaffung bei Dritten rechtfertigen können. Im Übrigen ist darüber hinaus jedenfalls an die allgemeine Bestimmung des Art. 4 DSchG zu erinnern, wonach eine Datenbearbeitung nur erfolgen darf, wenn eine gesetzliche Bestimmung

[53] S.o. III.

diese vorsieht oder wenn die (wohl gesetzlichen) Bestimmungen über die Erfüllung seiner Aufgabe es voraussetzen.

Vor dem Hintergrund dieser Anforderungen für die Beschaffung von Personendaten zumindest durch öffentliche Organe sind etwa zu detaillierte Fragebögen beim Eintritt in eine öffentliche Anstalt (etwa ein Altenheim oder eine Schule) immer dann nicht bzw. nur teilweise zulässig, wenn Angaben verlangt werden, die für die Wahrnehmung der in Frage stehenden öffentlichen Aufgabe nicht notwendig sind. Im Übrigen ist für eine solche Beschaffung von Daten eine gesetzliche Grundlage notwendig; die Einwilligung der Betroffenen genügt grundsätzlich nicht.

7. Datenbekanntgabe

Ebenfalls **besondere Vorschriften** bestehen für die **Datenbekanntgabe**. Diese stellt – etwa im Vergleich zu einer „amtsinternen" Bearbeitung – insofern einen weiteren Eingriff in die Persönlichkeitsrechte der Betroffenen dar, als auf diese Weise neben der eigentlich datenbearbeitenden Stelle Dritte (seien dies nun Private oder öffentliche Stellen) Einsicht in die bei der Behörde vorhandenen Daten erhalten. Vor diesem Hintergrund sind sowohl auf Bundesebene (Art. 19 DSG) als auch (in der Regel) auf kantonaler Ebene für die Bekanntgabe von Personendaten im Verhältnis zu den allgemeinen Regeln zusätzliche bzw. strengere Vorgaben zu beachten (wobei die allgemeinen Grundsätze aber ebenfalls zu beachten sind):

- Der **Anwendungsbereich des Art. 19 DSG** erstreckt sich sowohl auf den Datenaustausch zwischen Bundesorganen untereinander als auch auf die Weitergabe von Daten an kantonale, kommunale oder ausländische Behörden sowie an Privatpersonen.
- In materieller Hinsicht verlangt Art. 19 Abs. 1 DSG zunächst grundsätzlich eine **spezifische gesetzliche Grundlage**, so dass eine allgemeine gesetzliche Grundlage für die Datenbearbeitung wohl nicht genügt.
- Art. 19 Abs. 1 lit. a, b, c, d DSG sehen jedoch **Ausnahmen** von diesem Grundsatz vor (Weitergabe im Einzelfall zur Erfüllung einer gesetzlichen Aufgabe, Einwilligung im Einzelfall, allgemeine Zugänglichmachung der Daten durch die betroffene Person, unredliche Verweigerung der Bekanntgabe). Von besonderer praktischer Bedeutung dürfte die Ausnahme des Art. 19 Abs. 1 lit. a DSG sein, wonach die bekannt gegebenen Daten im Einzelfall zur Erfüllung einer gesetzlichen Aufgabe des Empfängers unentbehrlich sind.
- Besondere Vorgaben gelten für **Abrufverfahren**: Hier ist nach Art. 19 Abs. 3 DSG eine ausdrückliche gesetzliche Grundlage notwendig; soweit besonders schützenswerte Personendaten oder Persönlichkeitsprofile durch ein Abrufverfahren zugänglich gemacht werden, muss dies in einem formellen Gesetz ausdrücklich vorgesehen sein.

  Unter **Abrufverfahren** sind **automatisierte Verfahren** zu verstehen, die es dem informationssuchenden Organ ermöglichen, sich die gewünschte Information in einem existierenden Datenbestand selbst zu beschaffen bzw. eben „abzurufen", ohne dass die eigentlich bekannt gebende Behörde hier mitwirken

muss bzw. die Abrufung überhaupt bemerkt. Es liegt auf der Hand, dass mit solchen Verfahren besondere Risiken verbunden sind, kann hier doch definitionsgemäss nicht mehr jeder Einzelfall analysiert werden.

- Schliesslich ist Art. 19 Abs. 4 DSG zu beachten, wonach – selbst bei Vorliegen der Voraussetzungen für eine Bekanntgabe – die **Bekanntgabe zu verweigern oder einzuschränken** ist, wenn wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen einer betroffenen Person es verlangen oder wenn gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.

Art. 10, 11 DSchG enthalten im Wesentlichen parallele Vorgaben in Bezug auf die Bekanntgabe von Daten.

Zu beachten sind in diesem Zusammenhang auch die Vorgaben der Öffentlichkeitsgesetze,[54] die jedoch im Zusammenhang mit der Tätigkeit von Sozial- und Bildungsinstitutionen nur eher selten eine Rolle spielen dürften.

Eine Datenbekanntgabe eines öffentlichen Organs an eine Religionsgemeinschaft (z.B. die Übermittlung der Krankenhauseintritte von katholischen bzw. reformierten Patienten und Patientinnen an die jeweilige Pfarrei, damit ggf. Krankenbesuche stattfinden können) ist grundsätzlich nur im Falle des Bestehens einer gesetzlichen Grundlage oder einer Einwilligung im Einzelfall zulässig.

Fall 3 (Entscheid des Regierungsrates des Kantons Aargau v. 20.11.2002, AGVE 2002, 687 ff.):
X war in der Psychiatrischen Klinik Königsfelden hospitalisiert. Am 21.10.2001 nahm er sich dort das Leben. Am 4.12.2001 stellten die Eltern von X bei den Psychiatrischen Diensten des Kantons Aargau ein Gesuch um vollständige Akteneinsicht und um Zustellung der vollständigen Krankengeschichte des Verstorbenen. Hintergrund waren das persönliche Interesse an den Umständen des Todes von X sowie die Abklärung und Geltendmachung möglicher Haftpflichtansprüche gegen die Klinik bzw. die behandelnden Ärzte.
Das Datenschutzrecht regelt grundsätzlich nicht den postmortalen Persönlichkeitsschutz, so dass sich das Auskunftsrecht nicht auf das Persönlichkeitsrecht des Verstorbenen, das in Vertretung durch seine Erben bzw. Angehörigen ausgeübt wird, stützen kann. Ebensowenig und aus letztlich parallelen Gründen kann die Akteneinsicht aus Gründen des postmortalen Persönlichkeitsschutzes des Verstorbenen verweigert werden. Da die Datenschutzgesetzgebung nicht nur den Schutz des einzelnen Individuums verfolgt, sondern auch den Schutz der Rechtsgemeinschaft vor Übergriffen und Willkür von Datenbearbeitenden bezweckt, hat sich aber auch eine Bearbeitung von Daten Verstorbener auf eine gesetzliche Grundlage zu stützen, zumal die Bearbeitung von Daten Verstorbener mitunter die Persönlichkeitsrechte der Angehörigen betreffen kann.
Daher darf die Bekanntgabe der in Frage stehenden Daten grundsätzlich nur auf der Grundlage einer entsprechenden gesetzlichen Vorschrift erfolgen. Eine solche findet sich aber im kantonalen Recht nicht, da hier lediglich die Bearbeitung von Daten lebender Personen geregelt wird, während hinsichtlich des Rechts auf Einsicht in personenbezogene Daten Verstorbener eine echte Gesetzeslücke vorliegt.
Im Fall des Bestehens einer solchen Gesetzeslücke könnte die rechtsanwendende Behörde diese unter Rückgriff auf allgemein anerkannte Grundsätze bzw. eine in anderem Zusammenhang bestehende Regel schliessen. Gegen diesen, vom Regierungsrat vertretene Ansicht könnte jedoch aus methodischer Sicht jedenfalls im öffentlichen Recht eingewandt werden, dass damit letztlich das hier massgebliche Legalitätsprinzip ausgehebelt würde, könnte doch die rechtsanwendende Behörde unter Rückgriff auf „irgendwelche“ sonstwo vorhandene Regeln eine an sich notwendige gesetzliche Grundlage ersetzen. Gleichwohl erscheint das Vorgehen im konkreten Fall insofern vertretbar, als es nicht (mehr) um Personendaten geht und die Herausgabe der Akten von denjenigen Personen verlangt wurde, deren Persönlichkeitsrechte durch eine solche Bekanntgabe verletzt werden könnten.
Die Verordnung zum Bundesgesetz über den Datenschutz regelt – im Gegensatz zu dem in diesem Fall einschlägigen kantonalen Recht – die Bekanntgabe von Daten Verstorbener: Nach Art. 1 Abs. 7 VDSG ist über Daten Verstorbener Auskunft zu erteilen, wenn die Gesuchsteller ein Interesse an der Auskunft nachweist und keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen, wobei nahe Verwandtschaft und Ehe mit dem Verstorbenen ein Interesse begründet.
Allerdings könnte der Auskunftserteilung das Gebot der Wahrung des ärztlichen Berufsgeheimnisses (Art. 312 StGB) entgegenstehen. Eine Einwilligung des Verstorbenen war im konkreten Fall nicht ersichtlich. Das

[54] Hierzu, in Bezug auf die Bundesebene, EPINEY/CIVITELLA/ZBINDEN, Datenschutzrecht (Fn. 1), 50 ff.

ärztliche Berufsgeheimnis gilt auch nach dem Tod des Geheimnisberechtigten, und das Recht, Ärzte vom Berufsgeheimnis zu entbinden, ist höchstpersönlicher Natur, so dass die Erben nicht befugt sind, dieses Recht auszuüben, sind höchstpersönliche Recht doch unvererblich.
Allerdings kann die Aufsichtsbehörde nach der einschlägigen Bestimmung des kantonalen Gesundheitsgesetzes die Befreiung vom Berufsgeheimnis verfügen, dies allerdings nur, falls gegenüber dem Geheimhaltungsinteresse ein deutlich höherwertiges öffentliches oder privates Offenbarungsinteresse dies rechtfertigt, wobei die Verhältnismässigkeit zu wahren ist. Zwar können die Eltern von X durchaus ein Interesse (Geltendmachung von Haftpflichtansprüchen) geltend machen; jedoch ist es hierfür nicht erforderlich, dass sie die gesamte Krankenakte zur Kenntnis nehmen, in der im Übrigen in besonderem Masse schützenswerte höchstpersönliche Daten von X enthalten waren, welche den Ärzten während der Behandlung anvertraut wurden und die auch das Verhältnis zwischen dem Verstorbenen und seinen Angehörigen betreffen. Daher ist die Krankenakte lediglich einer ärztlichen Vertrauensperson zugänglich zu machen, der den Beschwerdeführern die für die Geltendmachung des Haftpflichtanspruchs notwendigen Angaben weiterleitet.

8. Auskunfts- bzw. Einsichtsrecht

Nach Art. 8 DSG, Art. 23 DSchG kann jede Person **Auskunft über die zu ihrer Person gespeicherten bzw. vorhandenen Daten** verlangen, ohne dass der Nachweis eines irgendwie gearteten Interesses erforderlich wäre. Adressat des Auskunftsrechts ist grundsätzlich der Inhaber der Datensammlung. Dies gilt auch, wenn er die Datensammlung durch einen Dritten bearbeiten lässt (Art. 10a DSG, Art. 23 Abs. 3 DSchG). Gegenstand des Auskunftsrechts sind alle Daten, die sich auf den Antragsteller beziehen sowie ggf. der Zweck der Bearbeitung, die Kategorien der bearbeiteten Dateien, die Kategorien der Beteiligten an einer Datensammlung und die Kategorien der Datenempfänger (vgl. auch Art. 8 Abs. 2 DSG). Im Übrigen enthält die einschlägige Gesetzgebung Vorgaben über die Modalitäten der Ausübung des Auskunftsrechts (Fristen, Kosten, usw.).
Das Auskunftsrecht kann aber auch **eingeschränkt** werden, wobei folgende Aspekte im Vordergrund stehen:

- **gesetzliche Verankerung** der Verweigerung des Einsichtsrechts (Art. 9 Abs. 1 lit. a DSG);
- Beeinträchtigung schutzwürder, überwiegender **Interessen Dritter** (Art. 9 Abs. 1 lit. b DSG, Art. 25 Abs. 1 lit. b DSchG);
- Beeinträchtigung überwiegender **öffentlicher Interessen** (Art. 9 Abs. 2 lit. a DSG, Art. 25 Abs. 1 lit. a DSchG).

Fall 4 (Verwaltungsgericht des Kantons Freiburg, Freiburger Zeitschrift für Rechtsprechung 2002, 427 ff.):
A und B sind die Eltern von X, der mit einer leichten Behinderung geboren wurde. Daher war zunächst streitig, ob X in einer Regelklasse eingeschult werden konnte. Nach mehreren schriftlichen und mündlichen Kontakten von A und B mit der Schulinspektorin und weiteren Behörden wurde letztlich die Entscheidung getroffen, X in der Regelklasse einzuschulen. Kurz vor dieser Entscheidung fand eine informelle Sitzung in der Anwesenheit von A und B, der Schulinspektorin sowie weiteren Behördenmitgliedern statt. Die Präsidentin der Schulkommission erstellte von der Sitzung eine Notiz, die sie der Schulinspektorin zustellte, die diese als vertraulich bezeichnete persönliche Notiz in das Schuldossier von X integrierte. A und B verlangten Einsicht in diese Notizen, was ihnen unter Hinweis auf den Charakter dieser Notizen als „persönliche Notizen“, die dem Einsichtsrecht – im Gegensatz zu einem eigentlichen Protokoll einer Sitzung (ein solches wurde nicht erstellt) – entzogen seien, verweigert wurde. A und B klagen gegen diese Verfügung und verlangen Einsicht in diese Notizen.

Wendet man das kantonale Datenschutzgesetz an,[55] so besteht nach Art. 23 Abs. 1, 2 DSchG ein Anspruch auf Einsicht bzw. Auskunft. Es geht hier um persönliche Daten von X, und A und B können (da X nicht urteilsfähig ist) für ihn Einsicht in das Dossier verlangen. Fraglich könnte noch sein, ob der Charakter der Notizen als „persönliche Notizen" hieran etwas ändert. Dies ist zu verneinen: Jedenfalls in dem Augenblick, in dem solche Notizen, unabhängig davon, ob sie als vertraulich oder persönlich bezeichnet werden, in ein bei einer Behörde vorhandenes Dossier integriert werden, ist die Datenschutzgesetzgebung anwendbar. Im Übrigen bezieht sich das Auskunftsrecht auch ganz allgemein auf alle, über eine Person bei der Behörde gespeicherten Personendaten, unabhängig davon, ob diese in ein „offizielles" Dossier integriert sind oder nicht; jede andere Lösung ermöglichte eine Relativierung, wenn nicht gar Aushebelung des Zugangsrechts, da die Behörde separate Dossiers anlegen und damit das Auskunftsrecht ins Leere laufen lassen könnte. Schliesslich sei nur am Rande in diesem Zusammenhang noch darauf hingewiesen, dass es hier keinesfalls um Daten geht, die eine Person ausschliesslich zum persönlichen Gebrauch bearbeitet (vgl. Art. 2 Abs. 2 lit. a DSG).

Allerdings kann die Auskunft nach Art. 25 Abs. 1 lit. a DSchG verweigert werden, wenn ein öffentliches Interesse dies verlangt. Hier könnte das öffentliche Interesse darin bestehen, dass die Schulbehörden ganz generell ein Interesse daran haben, dass die Schülerdossiers so viele Elemente wie möglich enthalten, damit es ihnen möglich ist, in allen Situationen adäquat und unter Berücksichtigung aller Umstände zu reagieren. Daher müssten möglichst viele Informationen über die Schüler an die Schulbehörden übermittelt werden, selbst solche Informationen, die als vertraulich bezeichnet werden. Wenn nun der Zugangsanspruch zu weit ist, könnte dieses öffentliche Interesse beeinträchtigt werden, da manche vertraulichen Informationen den Schulbehörden nicht mehr übermittelt würden und diese daher über möglicherweise wichtige Elemente in Unkenntnis wären. Dieses öffentliche Interesse könnte daher grundsätzlich schwerer wiegen als das Interesse des Einzelnen, solche Dokumente zu konsultieren. Vor diesem Hintergrund könnte also der Zugang zu solchen vertraulichen Informationen grundsätzlich verweigert werden. In diese Richtung argumentierte denn auch das kantonale Verwaltungsgericht, wobei es aber im Ergebnis im konkreten Fall der Notiz den vertraulichen Charakter absprach, auch unter Berücksichtigung einer Interessenabwägung.

Diese Argumentation des Verwaltungsgerichts vermag jedoch kaum zu überzeugen: Sie implizierte letztlich, dass bei der Interessenabwägung im Fall „vertraulicher Informationen" – wobei, wohl auch aufgrund der (irrigen) Anwendung des Verwaltungsrechtspflegegesetzes, das Verwaltungsgericht offenbar davon ausgeht, dass allgemein interne Verwaltungsdokumente, die im Hinblick auf die Entscheidfindung der Verwaltung produziert werden, dem Einsichtsrecht entzogen sind[56] – grundsätzlich kein Einsichts- bzw. Auskunftsrecht besteht, eine Annahme, die keinerlei Stütze im Datenschutzgesetz findet und auch darüber hinaus jedenfalls im Falle personenbezogener Daten nicht schlüssig erscheint. Das Datenschutzrecht geht nämlich von einem grundsätzlichen Einsichtsrecht aus, das lediglich – abgesehen von gesetzlich vorgesehenen Ausnahmen – auf der Grundlage einer konkreten Interessenabwägung eingeschränkt werden kann. Mit dieser Wertung steht es nicht im Einklang, dass es „vertrauliche", „persönliche" oder „interne" Notizen geben kann, bei denen die Interessenabwägung in gewisser Weise „vorgespurt" ist, so dass im Falle der Bejahung eines solchen Dokuments das Einsichtsrecht zumindest grundsätzlich zu verweigern ist. Vielmehr geht das Datenschutzrecht davon aus, dass grundsätzlich in jede bei der Behörde vorhandene Information, die Personendaten enthält, Einsicht genommen werden kann.[57] In Bezug auf die konkrete Konstellation ist es darüber hinaus höchst fraglich, ob bei Informationen über einen Schüler, die Teil seines Dossiers sind, überhaupt ein überwiegendes öffentliches Interesse bestehen kann, die Auskunft zu verweigern, zumal aus den vom Verwaltungsgericht angeführten Gründen: Denn das Interesse der Betroffenen auf Einsicht dürfte grundsätzlich schwer wiegen, geht es doch (zumindest potentiell) um ihre schulische Laufbahn. Weiter verhinderte die Ausübung des Auskunftsrechts auch nicht die Übermittlung von Informationen über die Schüler, die hiervon ja nicht betroffen ist, sondern führte lediglich dazu, dass die Betroffenen in die über sie gesammelten Angaben Kenntnis erlangen. Der Ansatz des Verwaltungsgerichts, das offenbar davon ausgeht, dass bestimmte vertrauliche Informationen über Schüler dann nicht mehr mitgeteilt würden, impliziert letztlich, dass diejenigen, die solche Informationen übermitteln, nicht zwingend hinter diesen stehen können, wenn sie mit den Betroffenen konfrontiert werden, eine Konstellation, bei der tatsächlich Vieles dafür spricht, dass solche Angaben eben tatsächlich nicht in das Dossier integriert werden

---

55 Das Verwaltungsgericht zog hingegen das Verwaltungsrechtspflegegesetz heran, dies wohl zu Unrecht, vgl. oben IV.2.

56 Ein Ansatz, der – wie noch dargelegt wird – dem Datenschutzrecht grundsätzlich fremd ist. Vgl. auch BGE 125 II 473 Erw. 4a), wo das Bundesgericht ausführt, das verfahrensrechtliche Akteneinsichtsrecht und das datenschutzrechtliche Auskunftsrecht seien selbständige Ansprüche, die hinsichtlich Umfang und Voraussetzungen nicht gleich seien.

57 Vgl. auch BGE 125 II 473 Erw. 4b), wo das Bundesgericht festhält, der Auskunftsanspruch nach Art. 8 DSG erstrecke sich auch auf Akten, die zwar von der Verwaltung als „intern" bezeichnet werden, die aber Angaben über den Gesuchsteller enthalten und diesem zugeordnet werden können.

sollten. Insofern führte der Auskunftsanspruch wohl nicht dazu, dass keine Informationen mehr übermittelt oder / und in das Schülerdossier integriert werden, sondern dazu, dass die Vertretbarkeit und Richtigkeit solcher Angaben seriös verifiziert werden, was ja nur begrüsst werden kann.
Nur am Rande sei in diesem Zusammenhang noch darauf hingewiesen, dass eine Einschränkung des Auskunftsrechts selbstredend dann in Betracht kommen kann, wenn seine Ausübung die interne Willensbildung der Behörde beeinträchtigen könnte, liegt doch in einem solchen Fall ein öffentliches Interesse vor, das die Reichweite des Auskunftsanspruchs einschränken kann (Art. 25 DSchG). Allerdings kann auf dieser Grundlage eine Verweigerung der Auskunft nur solange begründet werden, wie die interne Entscheidung noch nicht gefallen ist; ist das Verfahren – wie im vorliegenden Fall – abgeschlossen, kann auch die interne Meinungsbildung der Behörde durch die Herausgabe der Daten nicht mehr beeinträchtigt werden.[58] Im Übrigen verlangt es das Verhältnismässigkeitsprinzip, dass in Bezug auf die verschiedenen Informationen jeweils geprüft wird, ob die Entscheidfindung der Behörde tatsächlich beeinträchtigt werden kann.

VI. Schluss

Datenschutz wird häufig als „Effizienzhindernis“ für die Wahrnehmung bestimmter (öffentlicher) Aufgaben angesehen. Diese Feststellung ist durchaus im Grundsatz zutreffend, wäre es doch für die Behörden – um sich auf diese zu beschränken – am effizientesten, wenn möglichst viele Daten der Bürger und Bürgerinnen bei ihnen vorhanden wären und möglichst schrankenlos ausgetauscht werden könnten. In einem Rechtsstaat darf jedoch Effizienz grundsätzlich kein Kriterium dafür sein, als wesentlich eingestufte Errungenschaften eben dieses Rechtsstaats „ausser Kraft zu setzen“. Vielmehr ist der Rechtsstaat an sich teilweise (zumindest zunächst) ineffizient; man denke etwa – über die in diesem Beitrag angesprochenen Fragen hinaus – an die Vorgaben für ein faires Verfahren oder an die durch die Polizei zu beachtenden Vorschriften. Nur am Rande sei in diesem Zusammenhang bemerkt, dass der zunächst und zumindest teilweise nur anscheinend bestehende „Gewinn“ an Effizienz durch Abstriche bei der Beachtung rechtsstaatlicher Grundsätze sich durchaus zumindest mittelfristig in das Gegenteil verkehren kann, „profitiert“ der Staat doch von der Akzeptanz, die einem demokratischen Rechtsstaat seitens der Bürgerinnen und Bürger entgegen gebracht wird.
Im Übrigen bedeutet „richtig verstandener“ Datenschutz keineswegs, dass legitime öffentliche Interessen nicht verfolgt werden könnten. Vielmehr verpflichtet er die Behörden nur (aber immerhin), bei der Datenbearbeitung eine Reihe von letztlich aus Grundrechten und dem Rechtsstaatsprinzip ableitbaren Vorgaben zu beachten. Diese beinhalten einerseits verfahrensrechtliche Anforderungen i.w.S. (unter Einschluss des Erfordernisses der gesetzlichen Grundlage), andererseits gewisse materiellrechtliche Anforderungen insbesondere an den Umfang sowie die Art und Weise der Datenbearbeitung, die im Wesentlichen verhindern sollen, dass Daten „unnötig“ und „auf Vorrat“ bearbeitet werden, impliziert doch letztlich jede Datenbearbeitung eine Missbrauchsgefahr, die mit der Entwicklung der technischen Möglichkeiten steigt, ganz abgesehen davon, dass jede Bearbeitung von Personendaten einen Eingriff in das Grundrecht des Art. 13 BV darstellt. Vor

[58] Vgl. insoweit auch BGE 125 II 473, Erw. 4c).

diesem Hintergrund ist es m.E. durchaus möglich, den legitimen öffentlichen Interessen auf eine Bearbeitung von Personendaten Rechnung zu tragen, ohne rechtsstaatliche Grundsätze zu verletzen. Allerdings bedingt dies eine gewisse Sensibilität für die in diesem Beitrag dargelegten Vorgaben und durchaus gewisse Anstrengungen, die sich aber nach der hier vertretenen Ansicht im Hinblick auf die Wahrung rechtsstaatlicher Grundsätze sehr lohnen.